IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Application of:	§	Attorney Docket No. **GB920030011US1**
Gary Paul Noble	§	
	§	
Serial No.: **10/558,942**	§	Examiner: **Sarah Su**
	§	
Filed: **August 21, 2006**	§	Art Unit: **2431**
	§	
For: **METHODS, SYSTEMS AND**	§	Confirmation No.: **7231**
COMPUTER PROGRAM PRODUCTS	§	
FOR CONTROLLING THE	§	
DISCLOSURE TIME OF	§	
INFORMATION	§	

APPEAL BRIEF UNDER 37 C.F.R. 41.37

Mail Stop Appeal Briefs - Patents
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Sir:

This Appeal Brief is submitted in support of the Notice of Appeal filed October 13, 2010, in response to the final rejection of claims 1-5, 8-12, 16-20, and 22-24 in the Final Office Action (mailed July 23, 2010) for above-identified application.

REAL PARTY IN INTEREST

The real party in interest in the present Appeal is International Business Machines Corporation, the Assignee of the present application.

RELATED APPEALS AND INTERFERENCES

No appeals, interferences, or judicial proceedings are known to Appellant, the Appellant's legal representative, or Assignee, which may be related to, directly affect, or would be directly affected by or have a bearing on the Board's decision in the pending Appeal.

STATUS OF CLAIMS

Claims 1-5, 8-12, 16-20, and 22-24 remain present in this application. Claims 6, 7, 13-15, and 21 have been cancelled. Claims 1-5, 9-12, 19, 20, 23, and 24 stand finally rejected under 35 U.S.C. § 103(a) as being unpatentable over U.S. Patent No. 6,603,857 (hereinafter "Batten-Carew") in view of U.S. Patent Application Publication No. 2001/0052071 (hereinafter "Kudo"). Claim 8, 16-18, and 22 stand finally rejected under 35 U.S.C. § 103(a) as being unpatentable over Batten-Carew and Kudo in further view of U.S. Patent No. 6,813,358 (hereinafter "Di Crescenzo"). The rejection of claims 1-5, 8-12, 16-20, and 22-24 is appealed.

STATUS OF AMENDMENTS

No amendments have been entered (or offered) following the Final Office Action that led to this appeal.

SUMMARY OF CLAIMED SUBJECT MATTER

Independent claim 1 is directed to a method for controlling a disclosure time of information by a publisher to one or more recipients. With reference to Figs. 3b, and 4 (see page 8, line 3 through page 10, line 29, paragraphs [064]-[079]), the method includes a trusted body (30) generating an asymmetrical key pair for a specified date and time of disclosure with an encryption key and a decryption key (34). The trusted body (30) provides a digital certificate signed with a private key of the trusted body (30) to the publisher (10) prior to the specified date and time. The digital certificate provides the publisher (10) with the encryption key prior to the specified date and time (41). The publisher (10) uses the encryption key to encrypt data (42) and the recipient (31) obtains the encrypted data (44). The trusted body (30) makes the decryption key (34) available to the recipient (31) at the specified date and time (45). In this case, the trusted body (30) generates one or more asymmetrical key pairs for the specified date and time and a new asymmetrical key pair for each of a plurality of publishers (10). Each of the plurality of publishers (10) has a password issued by the trusted body (30) for preventing disclosure of the decryption key (34).

Independent claim 9 is directed to a system for controlling a disclosure time of information. With reference to Figs. 3b, and 4 (see page 8, line 3 through page 10, line 29, paragraphs [064]-[079]), the system includes a publisher (10), a trusted body (30), an asymmetrical key pair for a specified date and time of disclosure with an encryption key and a decryption key (34), and a digital certificate signed with a private key of the trusted body (30). The digital certificate provides the publisher (30) with the encryption key prior to the specified date and time. The system also includes means (which correspond to the trusted body (30)) for making the decryption key (34) available at the specified date and time. The publisher (10) includes a plurality of publishers (10). The asymmetrical key pair includes one or more asymmetrical key pairs for the specified date and time and a different asymmetrical key pair for each of the plurality of publishers (10). Each of the plurality of publishers (10) has a password issued by the trusted body (30) for preventing disclosure of the decryption key (34).

Independent claim 20 is directed to a method for controlling a disclosure time of information by a publisher to one or more recipients. With reference to Figs. 3b, and 4 (see page 8, line 3 through page 10, line 29, paragraphs [064]-[079]), the method includes a trusted body (30) generating an asymmetrical key pair for a specified date and time of disclosure with an encryption key and a decryption key (34). The method further includes the trusted body (30) providing the publisher (10) with the encryption key prior to the specified date and time. The method also includes the publisher (10) using the encryption key to encrypt data and the recipient obtaining the encrypted data. The trusted body (30) makes the decryption key (34) available to the recipient (31) at the specified date and time. The trusted body (30) generates one or more asymmetrical key pairs for the specified date and time, generating a new asymmetrical key pair for each of a plurality of publishers (10). Each of the plurality of publishers (10) has a password issued by the trusted body (30) for preventing disclosure of the decryption key (10).

Independent claim 23 is directed to a method for controlling a disclosure time of information by a publisher to one or more recipients. With reference to Figs. 3b, and 4 (see page 8, line 3 through page 10, line 29, paragraphs [064]-[079]), a computer program product directly loadable into the internal memory of a digital computer, comprising software code portions for performing the steps of claim 1 when said product is run on the digital computer. The method of claim 1 includes a trusted body (30) generating an asymmetrical key pair for a specified date and time of disclosure with an encryption key and a decryption key (34). The trusted body (30) provides a digital certificate signed with a private key of the trusted body (30) to the publisher (10) prior to the specified date and time. The digital certificate provides the publisher (10) with the encryption key prior to the specified date and time. The publisher (10) uses the encryption key to encrypt data and the recipient (31) obtains the encrypted data. The trusted body (30) makes the decryption key (34) available to the recipient (31) at the specified date and time. In this case, the trusted body (30) generates one or more asymmetrical key pairs for the specified date and time and a new asymmetrical key pair for each of a plurality of publishers (10). Each of the plurality of publishers (10) has a password issued by the trusted body (30) for preventing disclosure of the decryption key (34).

Independent claim 24 is directed to an information distributing service for controlling a disclosure time of information by a publisher to one or more recipients. With reference to Figs. 3b, and 4 (see page 8, line 3 through page 10, line 29, paragraphs [064]-[079]), the service includes a trusted body (30) generating an asymmetrical key pair for a specified date and time of disclosure with an encryption key and a decryption key (34). The trusted body (30) provides a digital certificate signed with a private key of the trusted body (30). The digital certificate provides the publisher (10) with the encryption key prior to the specified date and time. The publisher (10) uses the encryption key to encrypt data. The recipient (31) obtains the encrypted data and the trusted body (30) makes the decryption key (34) available to the recipient (31) at the specified date and time. The trusted body (30) is configured to generate one or more asymmetrical key pairs for the specified date and time, generating a new asymmetrical key pair for each of a plurality of publishers (10). Each of the plurality of publishers (10) has a password issued by the trusted body (30) for preventing disclosure of the decryption key (34).

GROUNDS OF REJECTION TO BE REVIEWED ON APPEAL

Whether claims 1-5, 9-12, 19, 20, 23, and 24 are patentable under 35 U.S.C. §103(a) over Batten-Carew in view of Kudo.

Whether claim 8, 16-18, and 22 are patentable under 35 U.S.C. § 103(a) over Batten-Carew and Kudo in further view of Di Crescenzo.

ARGUMENT

REJECTION OF CLAIMS 1-5, 8-12, 16-20, AND 22-24 UNDER 35 U.S.C. § 103(a)

At pages 3-12 of the Final Office Action, claims 1-5, 9-12, 19, 20, 23, and 24 were rejected under 35 U.S.C. § 103(a) over Batten-Carew in view of Kudo. The rejection of claims 1-5, 9-12, 19, 20, 23, and 24 under 35 U.S.C. § 103(a) is not well founded and should be reversed for at least the reason that the combination of Batten-Carew and Kudo does not teach or suggest all of the features set forth in Appellant's independent claims 1, 9, 20, 23, and 24. At pages 12-15 of the Final Office Action, claims 8, 16-18, and 22 were rejected under 35 U.S.C. § 103(a) over Batten-Carew and Kudo in further view of Di Crescenzo. The rejection of claims 8, 16-18, and 22 under 35 U.S.C. § 103(a) is not well founded and should be reversed for at least the reason that the combination of Batten-Carew, Kudo, and Di Crescenzo does not teach or suggest all of the features set forth in Appellant's independent claims. To establish *prima facie* obviousness of a claimed invention, all the claim limitations must be taught or suggested by the prior art. *In re Royka*, 490 F.2d 981, 180 USPQ 580 (CCPA 1974). "All words in a claim must be considered in judging the patentability of that claim against the prior art." In re Wilson, 424 F.2d 1382, 1385, 165 USPQ 494, 496 (CCPA 1970). If an independent claim is nonobvious under 35 U.S.C. § 103, then any claim depending therefrom is nonobvious. *In re Fines*, 837 F.2d 1071, 5 USPQ2d 1596 (Fed. Cir. 1988).

Independent Claims 1, 9, 20, 23, and 24

With respect to the rejection of independent claims 1, 9, 20, 23, and 24, Appellant submits that the combination of Batten-Carew and Kudo does not teach or suggest multiple publishers that each have a password issued by a trusted body for preventing disclosure of a decryption key. Appellant agrees that Batten-Carew discloses techniques for controlling the release of sensitive information that is encrypted with an encryption key and the generation of a decryption key (from a secret number that is released after a future time) for decrypting the encrypted sensitive information. Appellant also agrees that Batten-Carew discloses that the secret number may correspond to a private key (e.g., a decryption key) with a corresponding public key (e.g., an encryption key) being dependent thereon. Appellant further agrees that Batten-Carew does not teach or suggest a trusted body that provides a digital certificate signed with a private key of the trusted body to the publisher prior to a specified date and time, wherein the digital certificate provides the publisher with the encryption key prior to the specified date and time. However, Appellant does not agree that the combination of Batten-Carew and Kudo teaches or suggests multiple publishers that each have a password issued by a trusted body for preventing disclosure of a decryption key.

Appellant notes that Kudo paragraph [0003] discloses a communication between a user A and a user B in which a public encryption key of the user A, a name of the user A, and a digital signature of a certification authority (CA) are included in a certificate for the user A that is provided to the user B. As is disclosed, the user B obtains the certificate for the user A and confirms that the CA has provided the public encryption key for the user A. Assuming the digital signature is correct, the user B encrypts a target message for the user A with the public encryption key for the user A and sends the encrypted target message to the user A. In sum, Kudo paragraph [0003] merely discloses that providing the public encryption key of the user A (to the user B) in the form of a certificate ensures that the public encryption key actually belongs to the user A.

Moreover, Appellant does not agree that Kudo paragraph [0003], lines 4-10, discloses multiple publishers that each have a password issued by a trusted body for preventing disclosure of a decryption key. Kudo paragraph [0003] reads as follows:

> [0003] The use of a general certificate is shown in FIG. 1. When user B desires to encrypt data (M) and to transmit the encrypted data to user A, user B requests that a certification authority issue a certificate for user A. This certificate includes the name of user A and a public encryption key (KEa) for user A, and also the digital signature of the certification authority for all the contents. User B obtains the certificate for user A and confirms that the certification authority has provided the digital signature for the public encryption key for user A. If the digital signature is correct, user B encrypts the target message M by using the public encryption key (KEa) for user A, and transmits the encrypted message to user A.

More specifically, Kudo paragraph [0003] is directed to providing an encryption key to a user, as contrasted with a decryption key, passworded or otherwise. Furthermore, the 'name' is the name of the user that is to receive encrypted information and does not correspond to a password. In rejecting Appellant's argument, the Final Office Action (at page 3) states "…the claims do not provide further description of the password; therefore, the examiner has interpreted the name of Kudo as the password of the claimed invention." However, Appellant submits that the Examiner cannot ignore the plain meaning of the term 'password'. Moreover, Kudo's 'name' does not prevent disclosure of a decryption key. As noted above, Kudo paragraph [0003] discloses providing encryption keys to users, as contrasted with decryption keys and the Kudo 'name' corresponds to a name of user A (i.e., the name of the user that user B wishes to communicate with).

In rejecting Appellant's argument, the Final Office Action (at page 3) states "Kudo discloses that the decryption key is only transmitted to a particular user under certain conditions (0020, lines 10-12) and that the encrypted message is only transmitted if a digital signature of the particular user is verified (0003, lines 4-10). Kudo paragraph [0020] reads as follows:

> [0020] An encryption system according to the present invention is shown in FIG. 2. User B requests that a time-key certificate manager (hereinafter referred to simply as a time-key manager) issue a time-key certificate, including disclosure time information, and acquires it. Data to be transmitted to user A are encrypted by using a public key for encryption (KEt) included in the time-key certificate, and the encrypted data are transmitted. User A requests a decryption key from the time-key manager to decrypt the data received from user B. When the current time meets the decryption conditions, the decryption key is transmitted to user A, who can use it to decrypt the data.

With respect to Kudo paragraph [0020], Appellant agrees that Kudo discloses a time-key manager that transmits a decryption key to a user ‘A’, when a current time meets a decryption condition. However, Appellant submits that the digital signature of Kudo paragraph [0003] is the digital signature of the certificate authority that provides a public encryption key for an intended message recipient, and not a particular user. Moreover, Kudo paragraph [0020], similar to Batten-Carew, merely discloses preventing disclosure of encrypted information by not releasing a decryption key until after a future time and does not teach or suggest the use of a password that prevents disclosure of the decryption key.

For at least the reasons set forth above, Appellant respectfully submits that Appellant’s independent claims 1, 9, 20, 23, and 24 are allowable over the applied art of record (alone or in combination). Additionally, Appellant respectfully submits that dependent claims 2-5, 8, 10-12, 16-19, and 22 are also allowable for at least the reason that the claims depend on allowable claims.

CONCLUSION

The foregoing remarks also demonstrate that the applied art (alone or in combination) does not teach or suggest each feature of claims 1-5, 8-12, 16-20, and 22-24 as required to support a rejection under 35 U.S.C. § 103(a). Appellant therefore respectfully requests that the Board overturn the rejection of claims 1-5, 8-12, 16-20, and 22-24 under 35 U.S.C. § 103(a).

Appellant has submitted concurrently herewith the fee for the filing of this Appeal Brief. No additional fee is believed to be required. If, however, any additional fees are required, please charge those fees to IBM Corporation Deposit Account No. **09-0457**.

Respectfully submitted,

/Michael R. Long/
Michael R. Long
Reg. No. 42,808
DILLON & YUDELL LLP
8911 N. Capital of Texas Hwy., Suite 2110
Austin, Texas 78759
(512) 617-5521
ATTORNEY FOR APPELLANT

CLAIMS APPENDIX

1. A method for controlling a disclosure time of information by a publisher to one or more recipients comprising:

a trusted body generating an asymmetrical key pair for a specified date and time of disclosure with an encryption key and a decryption key;

the trusted body providing a digital certificate signed with a private key of the trusted body to the publisher prior to the specified date and time, the digital certificate providing the publisher with the encryption key prior to the specified date and time;

the publisher using the encryption key to encrypt data;

the recipient obtaining the encrypted data; and

the trusted body making the decryption key available to the recipient at the specified date and time, wherein the trusted body generates one or more asymmetrical key pairs for the specified date and time, generating a new asymmetrical key pair for each of a plurality of publishers, and each of the plurality of publishers has a password issued by the trusted body for preventing disclosure of the decryption key.

2. The method of claim 1, wherein the publisher verifies the signature on the digital certificate with the public key of the trusted body.

3. The method of claim 1, wherein the encryption key is a public key and the decryption key is another private key in a public key infrastructure.

4. The method of claim 1, wherein the trusted body creates the asymmetrical key pair for the specified date and time on demand from the publisher.

5. The method of claim 1, wherein the trusted body generates one key pair for the specified date and time.

6. (Cancelled)

7. (Cancelled)

8. The method of claim 1, wherein the decryption key is encrypted with a public key and only recipients with the corresponding private key can obtain the decryption key.

9. A system for controlling a disclosure time of information comprising:

a publisher;

a trusted body;

an asymmetrical key pair for a specified date and time of disclosure with an encryption key and a decryption key;

a digital certificate signed with a private key of the trusted body, the digital certificate providing the publisher with the encryption key prior to the specified date and time; and

means for making the decryption key available at the specified date and time, wherein there is a plurality of publishers, one or more asymmetrical key pairs for the specified date and time, a different asymmetrical key pair for each of the plurality of publishers, and each of the plurality of publishers has a password issued by the trusted body for preventing disclosure of the decryption key.

10. The system of claim 9, including one or more recipients with means for obtaining data encrypted with the encryption key from the publisher prior to the specified date and time and means for obtaining the decryption key at or after the specified date and time.

11. The system of claim 9, wherein the certificate includes the specified date and time, the encryption key, and a name of the trusted body.

12. The system of claim 9, wherein the encryption key is a public key and the decryption key is another private key in a public key infrastructure.

13-15. (Cancelled)

16. The system of claim 9, wherein the decryption key is encrypted with a public key and only recipients with a corresponding private key can obtain the decryption key.

17. The system of claim 9, wherein the trusted body has one or more agents who act on behalf of the trusted body.

18. The system of 9, wherein an agent for the trusted body is a smart card having an internal clock for providing the decryption key to a recipient.

19. The system of claim 10, wherein the trusted body is accessible by the publisher and the recipients via a communication network.

20. A method for controlling a disclosure time of information by a publisher to one or more recipients comprising:

a trusted body generating an asymmetrical key pair for a specified date and time of disclosure with an encryption key and a decryption key;

the trusted body providing the publisher with the encryption key prior to the specified date and time;

the publisher using the encryption key to encrypt data;

the recipient obtaining the encrypted data; and

the trusted body making the decryption key available to the recipient at the specified date and time;

wherein the trusted body generates one or more asymmetrical key pairs for the specified date and time, generating a new asymmetrical key pair for each of a plurality of publishers, wherein each of the plurality of publishers has a password issued by the trusted body for preventing disclosure of the decryption key.

21. (Cancelled)

22. The method of claim 20, wherein the decryption key is encrypted with a public key and only the recipient with a corresponding private key can obtain the decryption key.

23. A computer program product directly loadable into the internal memory of a digital computer, comprising software code portions for performing the steps of claim 1 when said product is run on the digital computer.

24. An information distributing service for controlling a disclosure time of information by a publisher to one or more recipients comprising:

a trusted body generating an asymmetrical key pair for a specified date and time of disclosure with an encryption key and a decryption key;

the trusted body providing a digital certificate signed with a private key of the trusted body, the digital certificate providing the publisher with the encryption key prior to the specified date and time;

the publisher using the encryption key to encrypt data;

the recipient obtaining the encrypted data; and

the trusted body making the decryption key available to the recipient at the specified date and time, wherein the trusted body is configured to generate one or more asymmetrical key pairs for the specified date and time, generating a new asymmetrical key pair for each of a plurality of publishers, and each of the plurality of publishers has a password issued by the trusted body for preventing disclosure of the decryption key.

EVIDENCE APPENDIX

None.

RELATED PROCEEDINGS APPENDIX

None.